braintrace™
INTELLIGENT CYBERSECURITY

1

Introductions

Dean Sapp, CISO

Braintrace, Inc.
220 S. 200 E., Suite 300
SLC, UT 84111
801-803-7902

Father of five great kids, student, author, security researcher, Spartan racer, and doer of hard things.

Security Certifications:

CISSP, CISA, CIPP/US, ITILv3, GCCC, GCIH, GSIP, GPEN, GAWN, GSLC, GCPM, GWAPT, G2700, GLEG, GSOC

2

UCIP CyberSecurity Risk Management

3

Top five cyber attacks we see causing losses

1. Business Email Compromise (BEC) / Wire Fraud
2. Ransomware attacks – **WannaCry/Petya/Others**
3. Unauthorized email and document access
4. Mobile phone compromise
5. Targeted social engineering

4

Sources

1. **2017 Verizon Data Breach Report (2016 findings)**
2. 2017 Cost of Data Breach Study: Ponemon Institute
3. 2016 Rand Institute, Cost and Causes of Cyber Incidents Report

verizon

5

Sources

1. 2017 Verizon Data Breach Report (2016 findings)
2. **2017 Cost of Data Breach Study: Ponemon Institute**
3. 2016 Rand Institute, Cost and Causes of Cyber Incidents Report

6

Sources

1. 2017 Verizon Data Breach Report (2016 findings)
2. 2017 Cost of Data Breach Study: Ponemon Institute
3. **2016 Rand Institute, Cost and Causes of Cyber Incidents Report**

RAND CORPORATION

7

Classic cons are still effective

	Incidents	Offenses	Victims	Known Offenders	Unknown Offenders
Total	5,428,613	5,856,985	5,845,031	4,078,106	2,025,419
Fraud Offenses					
False Pretenses/Swindle/Confidence Game	61,230	61,230	66,095	63,304	6,888
Credit Card/ATM Fraud	23,308	23,308	26,492	20,568	6,303
Impersonation	8,689	8,689	9,500	8,980	1,019
Welfare Fraud	1,289	1,289	1,300	1,344	27
Wire Fraud	984	984	1,074	808	281
Bribery	191	191	198	233	5
Counterfeiting/Forgery	91,697	91,697	110,545	85,797	21,201
Embezzlement	20,694	20,694	21,356	24,506	1,738
Arson + Fraud	10	20	5	23	0

Table 2 • Economic crime—Group A offenses

FBI Unified Crime Reporting lab statistics.

8

Classic cons have evolved

Many of the classic cons have been adapted to modern technology

- Get rich quick schemes
  - Nigerian Prince Scam – mail fraud
  - Current versions include ransomware & tax return fraud
- Persuasion tricks
  - Request for urgent business relationship or wire payments (BEC)
- Check fraud
  - Credit card fraud / ATM fraud
- Extortion
  - Webcam hacks and social media slander

Cyber crime is big business

- Cyber crime is growing at an alarming rate
  - Wire fraud / SWIFT client theft
    - In February, 2016 thieves attempted to steal $951 million from the Central Bank of Bangladesh. All but $81 million was recovered.
  - Business E-mail Compromise (BEC)
    - How does a BEC work?
    - The FBI recently calculated $3 billion in losses from US companies over the past few years from wire fraud.
  - Hacking at unprecedented levels
    - Estimated breach costs in 2015 exceed $39.1 billion.
    - Many companies never recover.

Almost everyone is a target

- What do the crooks really want?
  - All your monies! Preferably in **Bitcoin**
  - Or your stuff (inventory, used computers, devices, anything they can monetize)
  - **EFT/wires**/bank account numbers
  - Credit card numbers/health records
  - Intellectual property (Panama Papers…watch out law firms!)
    - copyrights
    - patents
    - trademarks
    - **mergers and acquisition data**
  - Insider trading information
  - Executive dossier (dôsē ˌā)

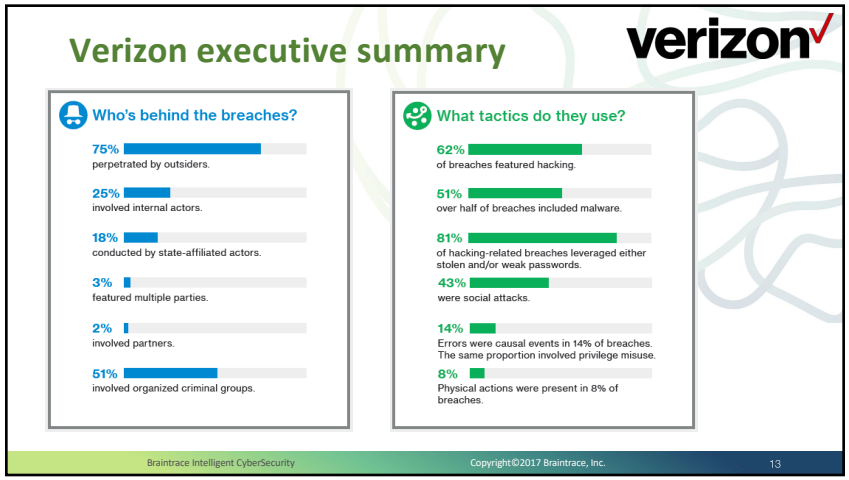
11

Verizon report contributors

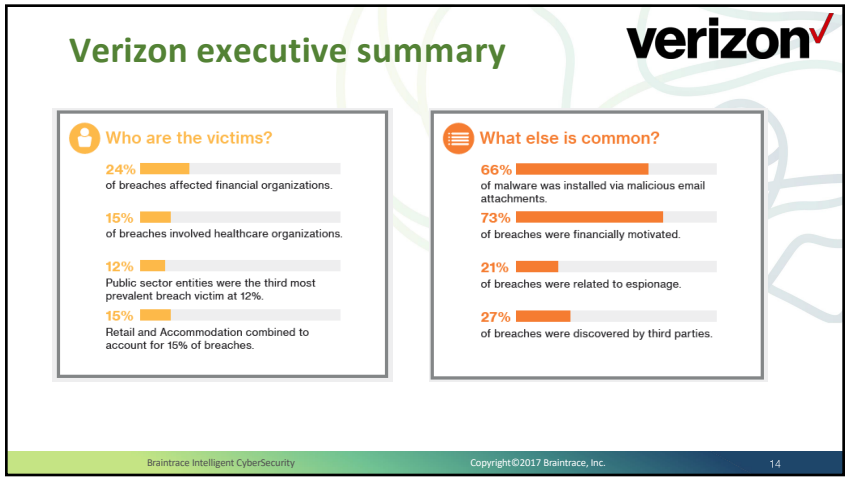
verizon

60+ agencies! Collaborating and sharing data!

12


Verizon executive summary
verizon
Who's behind the breaches?
75%
perpetrated by outsiders.
25%
involved internal actors.
18%
conducted by state-affiliated actors.
3%
featured multiple parties.
2%
involved partners.
51%
involved organized criminal groups.
What tactics do they use?
62%
of breaches featured hacking.
51%
over half of breaches included malware.
81%
of hacking-related breaches leveraged either stolen and/or weak passwords.
43%
were social attacks.
14%
Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.
8%
Physical actions were present in 8% of breaches.
Braintrace Intelligent CyberSecurity
Copyright©2017 Braintrace, Inc.
13

13


Verizon executive summary
verizon
Who are the victims?
24%
of breaches affected financial organizations.
15%
of breaches involved healthcare organizations.
12%
Public sector entities were the third most prevalent breach victim at 12%.
15%
Retail and Accommodation combined to account for 15% of breaches.
What else is common?
66%
of malware was installed via malicious email attachments.
73%
of breaches were financially motivated.
21%
of breaches were related to espionage.
27%
of breaches were discovered by third parties.
Braintrace Intelligent CyberSecurity
Copyright©2017 Braintrace, Inc.
14

14

Who was targeted in 2016?

verizon

	Incidents				Breaches			
	Total	Small	Large	Unk	Total	Small	Large	Unk
Manufacturing (31-33)	620	6	24	590	124	3	11	110
Mining (21)	6	1	1	4	3	0	1	2
Other Services (81)	69	22	5	42	50	14	5	31
Professional (54)	3,016	51	21	2,944	109	37	8	64
Public (92)	21,239	46	20,751	442	239	30	59	150
Real Estate (53)	13	2	0	11	11	2	0	9
Retail (44-45)	326	70	36	220	93	46	14	33
Trade (42)	20	4	10	6	10	3	6	1
Transportation (48-49)	63	5	11	47	14	3	4	7
Utilities (22)	32	2	5	25	16	1	1	14
Unknown	8,220	3	1,089	7,128	68	2	15	51
Total	42,068	606	22,273	19,189	1,935	433	278	1,224

15

Who was targeted in 2016?

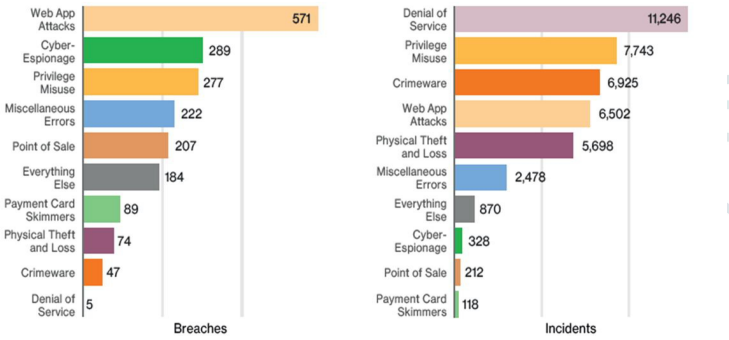
verizon

	Incidents				Breaches			
	Total	Small	Large	Unk	Total	Small	Large	Unk
Total	42,068	606	22,273	19,189	1,935	433	278	1,224
Accommodation (72)	215	131	17	67	201	128	12	61
Administrative (56)	42	6	5	31	27	3	3	21
Agriculture (11)	11	1	1	9	1	0	1	0
Construction (23)	6	3	1	2	2	1	0	1
Education (61)	455	37	41	377	73	15	15	43
Entertainment (71)	5,534	7	3	5,524	11	5	3	3
Finance (52)	998	58	97	843	471	39	30	402
Healthcare (62)	458	92	108	258	296	57	68	171
Information (51)	717	57	44	616	113	42	21	50
Management (55)	8	2	3	3	3	2	1	0

16

Incident classification patterns

verizon



17

Cost to a business

Ponemon INSTITUTE

According to the Ponemon Institute:

"In 2016, data breaches cost the most in the US and Germany… The average cost per capita of a data breach is **$225** per record…and the average total organizational cost in the US was **$7.35 million**."

-The most valuable individual records for the crooks to steal for identity theft purposes are medical records. They are also the most expensive breaches at $380 per record.

2017 Ponemon Breach Report

18

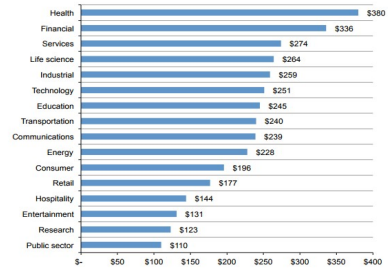
Cost per record in the U.S.

Ponemon INSTITUTE

Certain industries have higher data breach costs. Figure 4 reports the per capita costs for 16 industry sectors. Though a small sample size prevents us from generalizing industry cost differences, the pattern of industry results is consistent with previous research.

Specifically, heavily regulated industries such as health care, life science and financial services had a per capita data breach cost that is substantially above the overall mean of $225. In contrast, public sector (government), research and entertainment companies had a per capita cost well below the overall mean value.

Figure 4. Per capita cost by industry



2017 Ponemon Breach Report

19

Cost per breach in the U.S. ~ $200,000

Examining the Costs and Causes of Cyber Incidents

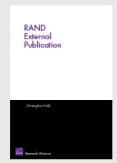
Published in: Journal of Cybersecurity, 2016

Posted on RAND.org on October 10, 2016

by Sasha Romanosky

Related Topics: Critical Infrastructure Protection, Cyber Warfare, Information Security

View related products



2016 RAND Breach Report

20

Cost per breach in the U.S. ~ $200,000

Cost of Cyber Incidents Not Large Compared with Other Business Losses; May Influence Responses by Businesses

FOR RELEASE
Tuesday
September 20, 2016

The cost of a typical cyber breach to an American company is much less than generally estimated, providing one possible explanation for why companies do not invest more to improve computer security, according to a new RAND Corporation study.

Researchers found that the typical cost of a breach was about $200,000 and that most cyber events cost companies less than 0.4 percent of their annual revenues. The $200,000 cost was roughly equivalent to a typical company's annual information security budget.

Media Resources

RAND Office of Media Relations
(703) 414-4795
(310) 451-6913
media@rand.org

Researcher Spotlight

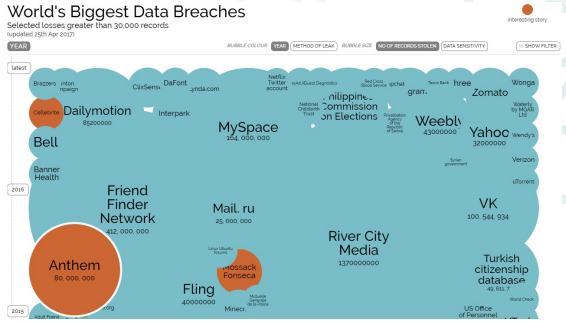
Sasha Romanosky
Policy Researcher

Sasha Romanosky is a policy researcher at the RAND Corporation and

2016 RAND Breach Report

21

Information is Beautiful



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

22

The 9 Largest Breaches – Huffington Post

9. The Home Depot (2014) – 56 Million records
8. Target (2013) – 70 Million Records
7. JP Morgan Chase (2014) – 76 Million records
6. Sony PSN (2011) – 77 Million records
5. Anthem (2015) – 80 Million records
4. TJX (2003) – 94 Million records
3. Heartland (2008) 130 Million records
2. eBay (2014) – 145 Million records
1. US business hacks (2012) – 160 Million records from multiple companies by one hacker group (victims included Nasdaq, JetBlue, JC Penny, 7-11 and many others)

Source: http://www.huffingtonpost.com

23

Total cost is hard to pinpoint

It may be a combination of detection and cleanup, victim recovery services and litigation expenses

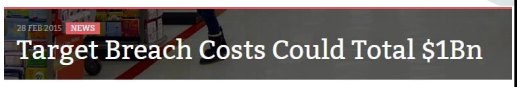
Anthem Agrees to $115 Million Settlement of Data Breach Lawsuit

By Bowdeya Tweh | Published June 23, 2017 | Features | Dow Jones Newswires

Target Breach Costs: $162 Million

Response Expenses Continue to Grow Following 2013 Incident

Jeffrey Roman (@gen_sec) · February 25, 2015 · 0 Comments



2016 RAND Breach Report

24

How much could it cost your business?

The only way to know with confidence is to get a cyber risk assessment completed

25

Attacks we see most often…

- BEC Email compromises
- Account / Password Theft
- Phishing Attacks
- Ransomware
- Attacks from missing patches
- IoT Attacks
- Mobile device compromise
- General hacking, whatever is easiest…

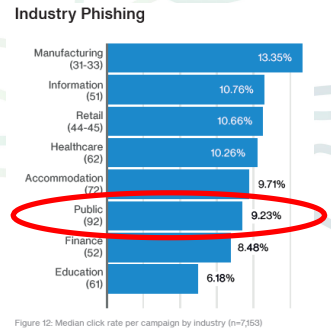


Figure 12: Median click rate per campaign by industry (n=7,153)

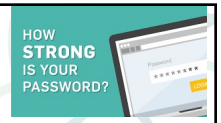
26

Business email compromise (BEC)

- Since 2013, 14,032 US companies have lost ~960M
  - Average loss of $68,415
- Since January 2015, 1,300% increase in losses
  - All 50 states, and 100 countries impacted.
  - Majority of the money going to banks in China.
- A large local financial company was targeted
  - Hacked the CEO's business email account
    - Sent an email with wire transfer instructions to Accounts Payable Manager.
    - Instructions to wire $175,000 over the weekend for an urgent and time sensitive deal.
    - Follow up email to wire an additional $240,000 to the same bank.

http://www.trigwire.com/state-of-security/latest-security-news/business-email-compromise-scams-have-cost-victims-3b-report-feds/_

Password theft / credential theft



- Passwords are the primary way attackers get into corporate networks
- Sometimes the hackers will just ask for user passwords…why work hard when you don't have too?
  - Would you give me your password for a piece of chocolate?
    - What about a candy bar?
    - Not even for some bacon?
    - What if I gave you 100 bucks? What about $25,000?
  - People will often give out their passwords
    - Including someone acting like the IT department, the help desk, or to the highest bidder.
    - If not, the hackers may try to guess them if they are short or simple.
    - Or they might just go search the dark web for a password that is common across personal and business accounts.

Phishing risks

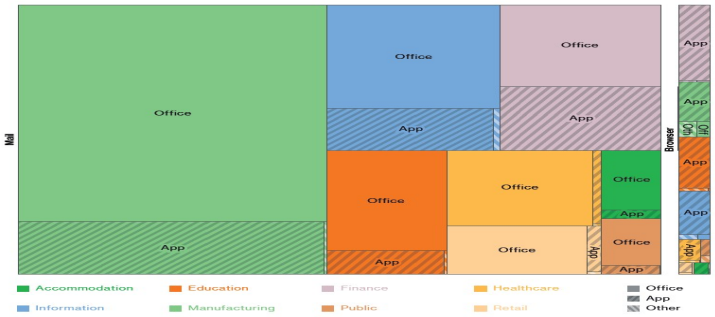
- If they can't guess your password, they likely will go phishing!
  - Phishing is the most successful way to compromise a computer and then gain access to a user's account and password
  - Dozens of phishing tools have been written to help the bad guys conduct phishing campaigns
  - Some phishing variants:
    - whaling
    - spear phishing (91% of the phishing attacks)
    - clone phishing
    - phone phishing (my nephew "Ugh…Uncle Dean, I need some help")
  - Results often include stolen passwords, ransomed computer, wire fraud, and potentially a cyber breach

29

Documents and Browsers!

verizon

Industry malware



30

Crime as a Service (CaaS)

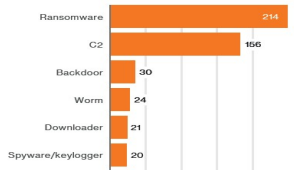
verizon

Crimeware

All instances involving malware that did not fit into a more specific pattern. The majority of incidents that comprise this pattern are opportunistic in nature and are financially motivated. This pattern will often affect customers and is where "typical" malware infections are placed.

At a glance

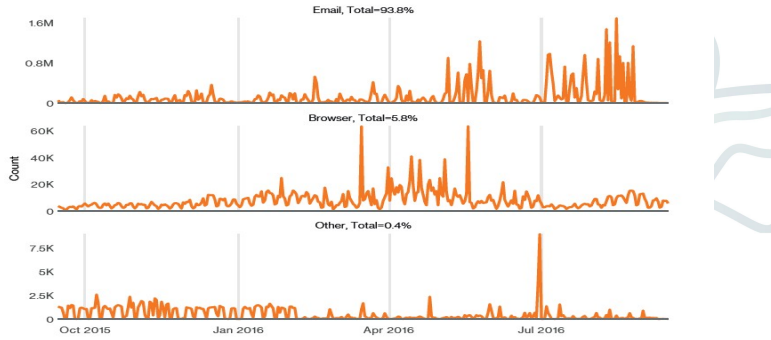
Top Industries
Public and Manufacturing
Frequency
6,925 total incidents, 47 with confirmed data disclosure
Key Findings
Ransomware has continued to increase for the last few years and is now the number one malware variety within this pattern. When examining non-incident data, 99% of malware is sent via email or webserver.



31

Crime as a Service (CaaS)

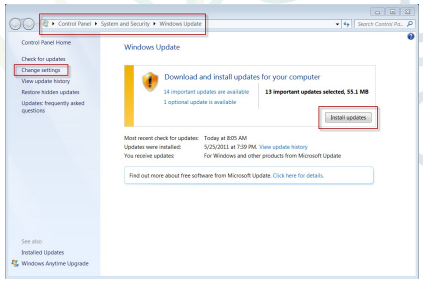
verizon



32

Missing Patches

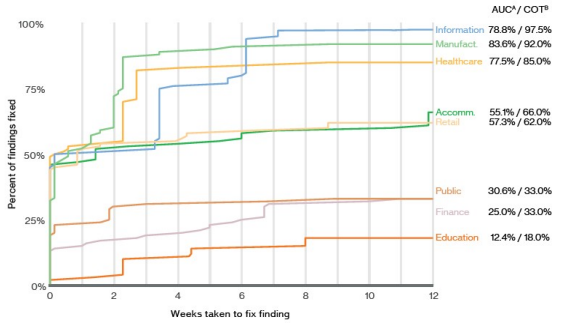
- If you have it on your network, patch it!
  - Computer Hardware
  - Computer Software
    - Operating Systems
    - Browsers
    - Plugins
    - Applications
  - SCADA systems
  - Firewalls, Routers
  - Websites
  - IoT Devices
  - Smart phones and Tablets
  - Printers



33

Patching is our Achilles' heel!

verizon

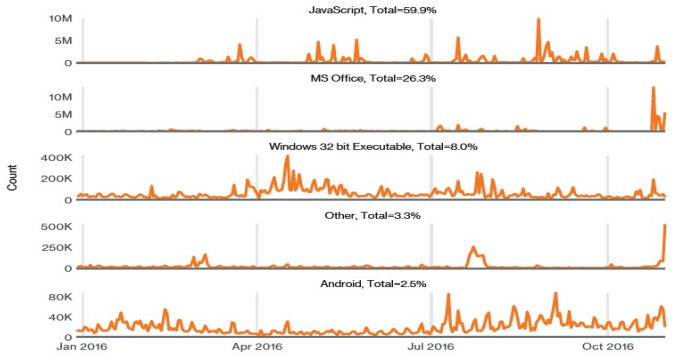


2017 Verizon Data Breach Reports

34

Threat areas to review

verizon



35

Five things to start doing tomorrow…

1. Harden your email systems
   a) Turn on DKIM, SPF, DMARC
   b) Digitally signing your email and quarantine unsigned emails for review
2. Lock down your firewall
   a) Block Blacklisted IPs (inbound and outbound)
   b) Geo-block if possible (inbound and outbound)
3. Secure your endpoints and servers
   a) Use a very good endpoint product with the security features enabled
   b) Turn on the local firewall, and turn off PowerShell and native tool access
4. Turn on multi-factor authentication for most valuable systems
   a) Especially email and systems to move money
5. Patch your stuff! Especially public facing systems!

36

What should we do over the next 12 months?

1. Get a cyber risk assessment and penetration test
2. Start using 2FA strong authentication for everything
3. Continue to patch your systems (especially public facing ones)
4. Consider managed security services
5. Deploy next generation endpoint protection
6. Set up an active breach detection system
7. Use a next-generation firewall
8. Encrypt your data and use offline backup options
9. Investigate CyberSecurity insurance options

37